MATH 433

Applied Algebra

Lecture 24:
More on algebraic structures.

Fields

Definition. A **field** is a set F, together with two binary operations called **addition** and **multiplication** and denoted accordingly, such that

- F is an Abelian group under addition,
- $F \setminus \{0\}$ is an Abelian group under multiplication,
- multiplication distributes over addition.

In other words, the field is a commutative ring with identity ($1 \neq 0$) such that any nonzero element has a multiplicative inverse.

Examples. • Real numbers $\mathbb{R}$.

- Rational numbers $\mathbb{Q}$.
- Complex numbers $\mathbb{C}$.
- $\mathbb{Z}_p$: congruence classes modulo p, where p is prime.
- $\mathbb{R}(X)$: rational functions in variable X with real coefficients.

Basic properties of fields

- The zero 0 and the unity 1 are unique.
- For any $a \in F$, the negative $-a$ is unique.
- For any $a \neq 0$, the inverse a^{-1} is unique.
- $-(-a) = a$ for all $a \in F$.
- $0 \cdot a = 0$ for any $a \in F$.
- $(-1) \cdot a = -a$ for any $a \in F$.
- $(-1) \cdot (-1) = 1$.
- $ab = 0$ implies that $a = 0$ or $b = 0$.
- $(a - b)c = ac - bc$ for all $a, b, c \in F$.

Vector space over a field

Definition. Given a field F, a **vector space** V over F is an additive Abelian group endowed with an action of F called **scalar multiplication** or **scaling**.

An **action** of F on V is an operation that takes elements $\lambda \in F$ and $v \in V$ and gives an element, denoted λv, of V.

The scalar multiplication is to satisfy the following axioms:

(V1) for all $v \in V$ and $\lambda \in F$, λv is an element of V;

(V2) $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;

(V3) $1v = v$ for all $v \in V$;

(V4) $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;

(V5) $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$.

Examples of vector spaces over a field F:

- The space F^n of n-dimensional coordinate vectors $(x_1, x_2, \ldots, x_n)$ with coordinates in F.
- The space $\mathcal{M}_{n,m}(F)$ of $n\times m$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- Any field F' that is an extension of F (i.e., $F \subset F'$ and the operations on F are restrictions of the corresponding operations on F'). In particular, $\mathbb{C}$ is a vector space over $\mathbb{R}$ and over $\mathbb{Q}$, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Characteristic of a field

A field F is said to be of nonzero characteristic if $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$ for some positive integer n. The smallest integer with this property is the **characteristic** of F. Otherwise the field F has characteristic 0.

The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ have characteristic 0.
The field $\mathbb{Z}_p$ (p prime) has characteristic p.

Since $(\underbrace{1 + \cdots + 1}_{n \text{ times}})(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = \underbrace{1 + \cdots + 1}_{nm \text{ times}}$, any nonzero characteristic is prime.

Any field of characteristic 0 has a unique structure of the vector space over $\mathbb{Q}$. Any field of characteristic $p > 0$ has a unique structure of the vector space over $\mathbb{Z}_p$. It follows that any finite field F of charasteristic p has p^n elements (where n is the dimension of F as a vector space over $\mathbb{Z}_p$).

Quadratic extension

Consider the set $\mathbb{Z}[\sqrt{2}]$ of all numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Z}$. This set is closed under addition, subtraction, and multiplication:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$
$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2},$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

It follows that $\mathbb{Z}[\sqrt{2}]$ is a ring. Actually, it is an integral domain. The quotient field of $\mathbb{Z}[\sqrt{2}]$ is $\mathbb{Q}(\sqrt{2})$, the set of all fractions $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, where $a, b, c, d \in \mathbb{Q}$ and $|c| + |d| \neq 0$. In fact, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$:

$$\frac{1}{c + d\sqrt{2}} = \frac{c - d\sqrt{2}}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{c}{c^2 - 2d^2} - \frac{d}{c^2 - 2d^2}\sqrt{2}.$$

The field $\mathbb{Q}[\sqrt{2}]$ is a **quadratic extension** of the field $\mathbb{Q}$. Similarly, the field $\mathbb{C}$ is a quadratic extension of $\mathbb{R}$, $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

Algebra over a field

Definition. An **algebra** A over a field F (or F-**algebra**) is a vector space with a multiplication which is a bilinear operation on A. That is, the product xy is both a linear function of x and a linear function of y.

To be precise, the following axioms are to be satisfied:

(A1) for all $x, y \in A$, the product xy is an element of A;
(A2) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for $x, y, z \in A$;
(A3) $(\lambda x)y = \lambda(xy) = x(\lambda y)$ for all $x, y \in A$ and $\lambda \in F$.

An F-algebra is **associative** if the multiplication is associative. An associative algebra is both a vector space and a ring.

An F-algebra A is a **Lie algebra** if the multiplication (usually denoted $[x, y]$ and called **Lie bracket** in this case) satisfies:

(Antisymmetry): $[x, y] = -[y, x]$ for all $x, y \in A$;
(Jacobi's identity): $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in A$.

Examples of associative algebras:

- The space $\mathcal{M}_n(F)$ of $n \times n$ matrices with entries in F.
- The space $F[X]$ of polynomials
$p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- The space of all functions $f : S \to F$ on a set S taking values in a field F.
- Any field F' that is an extension of a field F is an associative algebra over F.

Examples of Lie algebras:

- $\mathbb{R}^3$ with the cross product is a Lie algebra over $\mathbb{R}$.
- Any associative algebra A with a Lie bracket (called the **commutator**) defined by $[x, y] = xy - yx$.